REMARKS

I. Status of Claims

The Applicant has carefully considered the Office Action dated October 15, 2008, and the references it cites. Currently, claims 1-12 are pending. In the Office Action, claims 1-5 and 7-10 were rejected under 35 U.S.C. § 103(a) as being obvious over 3rd Generation Partnership Project, "Document 2: KASUMI Specification" Release 4 (*DKS*) in view of U.S. Patent No. 6,324,288 (*Hoffman*) and in further view of "Parallel Stream Cipher for Secure High-Speed Communication" to Lee (*Lee*). Further, the Examiner objected to claims 6, 11, and 12 and indicated the claims would be allowable if rewritten in independent form to include the base claim and any intervening claims.

In response, the Applicant submits the following remarks.

II. Claim Rejections Under 35 U.S.C. § 103(a)

Claim 1 recites an encryption method for dividing a first plaintext bit stream of length 2n into first and second sub-bit streams of length n and dividing a second plaintext bit stream of length 2n into third and fourth sub-bit streams of length n, the method comprising, *inter alia*, performing a first-round of encryption by encrypting the received the first and second sub-bit streams with predetermined first encryption codes an odd number of times, and outputting the second ciphertext bit stream encrypted again with a predetermined time delay right after the first ciphertext bit streams of length n are outputted, generating a first operated ciphertext bit stream, generating a second operated ciphertext bit stream, and performing a second-round of encryption by encrypting the received first operated ciphertext bit stream comprising concurrently outputting the third and fourth ciphertext bit streams.

The Applicant submits that *KDS* does not describe dividing a second plaintext bit stream of length 2n into third and fourth sub-bit streams of length n. To allege that *KDS* describes the first plaintext bit stream, the Examiner cites to FIG. 1. Presumably, the Examiner contends the 64-bit input corresponds to the first plaintext bit stream and the key used encrypt the 64-bit input corresponds to the second plaintext bit stream. However, "KASUMI is a block cipher that produces a 64-bit output from a 64 bit input under the

control of a 128-bit key." *See KDS at p. 8, § 6.1.* In other words, the Examiner alleges that the length of the first and second sub-bit streams is 32 bits and the length of the third and fourth sub-bit streams is 64 bits. Thus, the sub-bit streams described in *KDS* do not have the same length. Accordingly, *KDS* is not analogous to claim 1, which recites dividing a first plaintext bit stream of length 2n into first and second sub-bit streams of length n and dividing a second plaintext bit stream of length 2n into third and fourth sub-bit streams of length n.

Further, the Applicant submits that *KDS* does not describe a predetermined delay. In rejecting claim 1, the Examiner contends that in figure 2 of *KDS*, a "predetermined time delay always takes place wherever there is a requirement to synchronize two inputs compute an 'exclusive OR' functions [sic]." *See the Office Action at p. 12, ll. 17-19.* However, in figure 2 of *KDS*, there are different time delays associated with its operation. For example, the first FIi1 function must wait for completion of the XOR function (using $KO_{I,1}$). However, the XOR function immediately after the FIi1 function must wait for the completion of the FIi1 function and the first XOR function. Thus, the first XOR function must wait a first time period, and the second XOR function must wait a second time period that is different from the first time period. In contrast, claim 1 recites outputting the second ciphertext bit stream encrypted again with a predetermined time delay.

Further, the Examiner's allegations regarding the background section of the patent application are in error. Specifically, the Applicant notes the MPEP sets forth that the specification of a patent application normally encompasses a background of the invention that "describ[es] to the extent practical the state of the prior art or other information disclosed known to the applicant[.]" *See MPEP § 608.01(c) (emphasis added).* In the background of the present application, a detailed explanation of the conventional art that is implemented by the Applicant is provided for the Examiner's convenience and the Examiner incorrectly construes it to be admitted prior art.

The Applicant further submits that no motivation to combine the descriptions of *KDS* and *Lee* as the Office Action contends. In rejecting claim 1, the Examiner alleges that it would be obvious to combine the teachings of *KDS* and *Lee* to optimize the speed. However, in making this alleged combination, the Examiner contends that *Lee* describes performing encryption of first and second ciphertext bit streams at the same time. The Examiner's reading of *Lee* is overbroad because it specifically describes a keystream generator that

"generates independent sequences from nonlinear combine functions[.]" *See Lee at p. 262, § 2.3, para. 1.* Further, as noted in figure 3 of *Lee*, the generated key is used to decipher the ciphertext and, thus, does not describe performing encryption of first and second ciphertext bit streams at the same time.

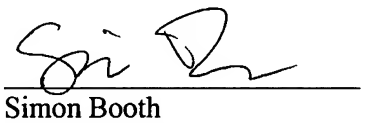
In addition, it is not possible to make the alleged combination because, in *KDS*, the FO function is recursive and requires the first ciphertext bit stream in order to complete the second alleged round. Specifically, as noted in figure 2 of *KDS*, the encrypting at FIi2 requires the output of FIi1. Thus, there is no reason to make the alleged combination because the operation of FIi2 must follow the operation of FIi1. Stated differently, the Examiner assumes that the operation of the FO function in KDS is linear and can be parallelized by splitting the function into two separate, but equal functions. But recursive functions such as a factorial function cannot simply be parallelized. For example, by the Examiner's contentions, the factorial of 6 is equal to the sum of two factorials of three (i.e, $6! = 3! + 3!$). However, the factorial of 6 is equal to 720, and the sum of the factorials of 3 is 12. Accordingly, it is not possible to make the alleged combination because the result would be inoperable and, thus, there is no reasonable expectation of success. *See MPEP § 2143.02.*

None of the cited prior art, either alone or in combination, cure the deficiencies of *KDS* and *Lee*. Thus, for at least the foregoing reasons, claim 1 and all claims depending therefrom are in condition for allowance and notice to that effect is respectfully requested. Independent claim 8 and all claims depending therefrom are also patentable for at least substantially the same reasons discussed above in connection with claim 1.

III. Conclusion

The Applicant submits that the above amendments and arguments are fully responsive to the Office Action dated October 15, 2008. Further, the Applicant submits that, for at least the foregoing reasons, all pending claims are in condition for allowance and notice to that effect is requested. Should the Examiner have any questions, the Examiner is encouraged to contact the undersigned at the telephone number indicated below.

Respectfully submitted,



Simon Booth
Attorney of Record
Reg. No. 58,582

Roylance, Abrams, Berdo & Goodman, L.L.P.
1300 19th Street, N.W., Suite 600
Washington, D.C. 20036-2680
(202) 659-9076

Dated: December 12, 2008